Network Computing Darkreading

Welcome Guest

Login to your account

Register

Advertise

About Us

SECTIONS

- Authors
- Slideshows
- Video
- Reports
- White Papers
- Events
- Black Hat
- Attacks/Breaches
- App Sec
- Cloud
- Endpoint
- Mobile
- Perimeter
- Risk
- Operations
- Analytics
- Vulns/Threats
- Threat Intelligence
- Careers and People
- IOT

- Login to your account
- Register
- About Us
- Advertise

Search Dark Reading

- Facebook
- Twitter
- LinkedIn
- Google+
- RSS

Want to build an **Information Security** *Awareness program that works?* LEARN HOW HERE TERRANOVA

DARKReading

Join us live at Interop ITX

Search Dark Reading

Analytics
Attacks / Breaches
App Sec
Careers & People
Cloud
Endpoint
IoT
Mobile
Operations
Perimeter
Risk
Threat Intelligence
Vulns / Threats

Vulnerabilities / Threats

2/18/2014
11:35 AM

Mathew J. Schwartz
News

6 comments
Comment Now

Login

50%50%

Like Tweet Share G+

Bye, Bitcoin: Criminals Seek Other Crypto Currency

Law enforcement crackdowns, hack attacks, and market volatility drive Russian fraudsters to mint their own virtual currency systems.

When it comes to profiting from ill-gotten gains, have bitcoins become *passé*?

That appears to be the prevailing attitude on some leading Russian cybercrime forums, which have ditched well-known virtual currencies -- including Perfect Money and Bitcoin -- in favor of forum-specific alternatives, which administrators claim offer higher levels of anonymity, security, and reliability.

Blame the shift, at least partly, on the Justice Department's takedown of Liberty Reserve, which was a Costa Rica-based virtual currency system that sported one million users. After it was closed, criminals needed to find new ways to move money and store stolen funds -- preferably without having their profits picked off by either rivals or investigators. "Ever since the Liberty Reserve takedown in May of last year and the confiscation of all accounts by law enforcement, fraudsters have been busy finding a solid currency to which they can entrust their spoils without the risk of losing them in a bust," said RSA fraud intelligence analyst Daniel Cohen in a blog post.

Why not simply use existing virtual currency options? While Perfect Money and Bitcoin would seem to be "the obvious choices" for cybercriminals, said Cohen, "Perfect Money is of questionable background, while Bitcoin does not provide fraudsters the required level of anonymity and is not immune to seizure." For example, US prosecutors in November seized bitcoins worth more than $34.1 million from users of the "darknet" narcotics marketplace known as Silk Road.

[Target's breach has driven propoals for new ways to exchange funds, but none hit the bull's-eye. Learn Why Alternate Payment Schemes Get No Love.]

Criminals also risk having their bitcoin hordes stolen by rivals. Last week, for example, the administrator of a darknet site known as Silk Road 2 -- which, like its namesake, serves as a marketplace for buying and selling narcotics -- said that the site had been hacked, and all of its users' bitcoins stolen, the BBC reported.

According to a forum post from a Silk Road 2 administrator (who goes by "Defcon"), one of the site's vendors made off with the bitcoin haul -- worth an estimated $2.7 million -- by exploiting a recently discovered vulnerability involving transaction malleability. The heist led a number of bitcoin exchanges to suspend operations until they bolster their defenses. "I should have taken MtGox and Bitstamp's lead and disabled withdrawals as soon as the malleability issue was reported. I was slow to respond and too sceptical (sic) of the possible issue at hand," Defcon said in a forum posting.

Those bitcoin exchange suspensions have recently driven the value of a bitcoin to less than $300 on Mt Gox -- which typically handles about one-fifth of the world's bitcoin trades -- compared to the currency being valued Tuesday on other exchanges at about $630. Still, that's down from the $1,200 commanded by a bitcoin back in November.

That market volatility is likely another reason why many criminals have opted for an alternative cryptographic currency, digital currency expert Michael Jackson, a former COO at Skype, told The Register. "It suggests that criminals don't trust Bitcoin -- I hope this is because they think the police will find them, but I suspect it's more to do with the fact that they don't like volatility. Even an online dope seller wants predictability in his business."

Photo credit: zcopley.

Sponsored Content
The Ransomware Survival Handbook
A guide to prevention, response, and recovery
Brought to you by Barkly

What's arguably even better for criminals, however, is anonymity. "Buyers and sellers of crimeware services have long had anonymous handles with which to do business," said Sean Sullivan, security advisor at F-Secure Labs, via email. "Anonymity has allowed crimeware to evolve into a highly commoditized ecosystem. Having its own currency system adds another layer of anonymity."

Cybercriminals, however, are likely still using bitcoins for some purposes. "They probably aren't avoiding bitcoins other than when it comes to buying and selling crimeware services," Sullivan said. "They are all probably invested in Bitcoin in order to move and launder 'real' money."

What's on offer for criminals seeking Bitcoin and Perfect Money alternatives? To date, RSA said it's been tracking three Russian-built currency systems -- MUSD, United Payment System, and UAPS -- all of which are tailor-made to help criminals evade law enforcement agencies. "These new internal currencies are carefully administered and secured, ensuring a high level of anonymity in transaction and hiding the user identities, making it more difficult for law enforcement to trace, block, or seize funds and accounts," RSA's Cohen said. The services allow users to deposit funds and cash out their holdings, sometimes to a prepaid credit card.

So far, the most advanced option appears to be UAPS -- a.k.a. the "First Commercial Bank" -- which first appeared more than a year ago on a Russian cybercrime forum. The currency system reportedly sports its own development team, gets frequent updates, and, per its data-retention policy, holds related data for only two months before purging it from the system.

Four different cybercrime boards, meanwhile, appear to have standardized on the United Payment System currency system. According to RSA, each board has its own exchange agent, who's overseen by a site administrator charged with keeping the dealings "honest." That approach highlights how cybercrime forums rely on members to stay straight with each other. "Doing business with crimeware suppliers is based on trust -- karma systems, feedback -- like [on] eBay," Sullivan said. "Buyers rate sellers. A currency provider will have to earn trust -- and heaven help him if he breaks that trust with a large number of cybercriminals."

The MUSD currency first appeared in November 2013. It's only being used on one forum, and it allows users to buy or sell services, as well as procure forum advertising. The currency's developers say their system offers anonymity, a built-in escrow service, and the ability to cash out the currency in person. "Two verified exchange agent services currently work with MUSD in this board, with one offering to cash out MUSD for hard currency in person at an office in Kiev, Ukraine," said Cohen.

On a related note, Russian authorities have recently been signaling that they'll crack down on users of any type of virtual currency, including bitcoins. "Citizens and legal entities risk being drawn -- even unintentionally -- into illegal activity, including laundering of money obtained through crime, as well as financing terrorism," according to a warning issued last month by Russia's central bank.

Earlier this month, Russian authorities warned that only rubles are legal tender inside Russia, and that trading in bitcoins is illegal. "Systems for anonymous payments and cybercurrencies that have gained considerable circulation -- including the most well-known, Bitcoin -- are money substitutes and cannot be used by individuals or legal entities," according to a statement by the Russian Prosecutor General's Office.

The NSA leak showed that one rogue insider can do massive damage. Use these three steps to keep your information safe from internal threats. Also in the Stop Data Leaks issue of Dark Reading: Technology is critical, but corporate culture also plays a central role in stopping a big breach. (Free registration required.)

Mathew Schwartz served as the InformationWeek information security reporter from 2010 until mid-2014. View Full Bio

Comment | Email This | Print | RSS

More Insights

Webcasts

Your Toughest AppSec Questions Answered

Cybersecurity Crash Course - Session 7: Security For IoT

More Webcasts

White Papers

8 Nation-State Hacking Groups to Watch in 2018

The Main AppSec Tech to Adopt in 2018

More White Papers

Reports

[Forrester's Report] The State of Application Security: 2018 & Beyond

[Dark Reading Report] Navigating the Threat Intelligence Maze

More Reports

Comments

Newest First | Oldest First | Threaded View

s404n1tn0cc,
User Rank: Apprentice
2/20/2014 | 9:14:34 AM

Login
100% 0%

So much for Law proofing.

Seems sence the US invented the Ethernet it owns it and all Backdoors. Obviously they some how where able to get subpoenas. And direct access to the accounts. but when they did that the 34000000 dollars is now worth only 8500000. A tremendous shock to the system.

Reply | Post Message | Messages List | Start a Board

asksqn,
User Rank: Ninja
2/19/2014 | 9:04:08 PM

Login
0% 100%

Bitcoin, We Hardly Knew Ye

Notwithstanding the negative nellie approach to cryptocurrencies, Bitcoin will always be remembered for causing the widespread soiling of jockey shorts worn by members of the Federal Reserve, Greenspan, Bernanke and other keepers of the fiat money cartel.

Reply | Post Message | Messages List | Start a Board

Thomas Claburn,
User Rank: Ninja
2/18/2014 | 6:49:07 PM

Login
0% 100%

Re: Why tie to physical location?

It would be fitting if cybercriminals took to using actual cans of Hormel Spam as currency.

Reply | Post Message | Messages List | Start a Board

Brian.Dean,
User Rank: Apprentice
2/18/2014 | 4:06:59 PM

Login
0% 100%

Re: Why tie to physical location?

This is one area where technology is not being used for the good of society. The easiest way to limit illegal activities is by limiting/restricting free movement of finance. However, it is not all negative as technology that enables agencies to detect narcotics using sensors etc restores some of the balance.

I feel since Bitcoin is not doing too good even for legal activities, I wonder whether another crypto currency will every gain the kind the hype and value that Bitcoin gained during the month of November last year.

Reply | Post Message | Messages List | Start a Board

Mathew,
User Rank: Apprentice
2/18/2014 | 12:30:52 PM

Login
50%50%

Re: Why tie to physical location?

Good question. These are add-ons to Russian-language cybercrime forums. It doesn't mean that the admins or users reside in Russia. But if they do, they might want a way to cash out large amounts of money in rubles, for local spending.

Reply | Post Message | Messages List | Start a Board

Lorna Garey,
User Rank: Ninja
2/18/2014 | 12:00:58 PM

Login
50%50%

Why tie to physical location?

Mat, why would a group looking to launch a cyber-currency tie itself to a specific country, especially Russia? The U.S., EU and China also seem like bad bets. It's CYBER after all, so why not be completely separate from any physical location?

Reply | Post Message | Messages List | Start a Board

Related Content Sponsore

RESOURCES VIDEOS BLOG WEBINAR

NSS Labs’ Breach Prevention Summary Report

NSS Labs' Breach Prevention Summary Report presents test results for Check Point's 15600 Next Generation Threat...

The Next Attack Can Be Prevented

This white paper delivers fresh insights into how cyber threats have intensified. Building on this analysis, the white paper gives practical recommendations for improving

Cyber-Attack Security Guide

Cyber Security with Intention, An Executive Guide gives C-level executives and other decision makers high-level explanations of cyber security issues, misconceptions,

Ransomware Can Be Prevented

Ransomware is today's fastest growing and most destructive type of cyber-attack. This white paper gives readers a detailed understanding of ransomware...

Customer Testimonials: Mississippi Secretary of State Gains End to End Advanced Threat Protection for Its Data

The Mississippi Secretary of State sought protection against advanced...

Hot Topics Editors' Choice

5 Threats from Mobile Ransomware & Banking Malware Are Growing

Jai Vijayan, Freelance writer, 2/26/2018

2
[Security Starts with the User Experience]
Peter Hesse, Chief Security Officer at 10Pearls, 2/27/2018

1
[SAML Flaw Lets Hackers Assume Users' Identities]
Kelly Sheridan, Associate Editor, Dark Reading, 2/27/2018

Subscribe to Newsletters

Live Events Webinars

TI + Orchestration = OODA Loop Acceleration

Your Toughest AppSec Questions Answered

Cybersecurity Crash Course - Session 7: Security For IoT

Webinar Archives

White Papers

[8 Nation-State Hacking Groups to Watch in 2018]

[GDPR - Friend or Foe?]

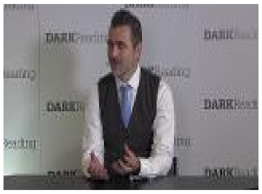
[Minimze App Security Risks With DevOps]

[The Equifax Breach & How Software Composition Analysis Cloud Have Prevented It]

[The Main AppSec Tech to Adopt in 2018]

More White Papers

Video



How Security Metrics Fail

Attacking De

All Videos

Cartoon Contest

Write a Caption, Win a Starbucks Card! [Click Here]

Latest Comment: [I tried to tell him he was taking on too much.]

Cartoon Archive

Current Issue

How to Cope with the IT Security Skills Shortage

Most enterprises don't have all the in-house skills they need to meet the rising threat from online attackers. Here are some tips on ways to beat the shortage.

Download This Issue!

Back Issues | Must Reads

Flash Poll

Has the U.S. political climate caused you to make infosecurity-related changes to your disaster recovery/business continuity plans?

○ Yes

○ No

○ No but we are considering it

○ Still waiting for cybersecurity guidance from Trump admin EO

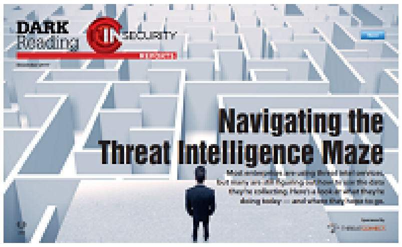
○ Don't know

○ Other (Please explain in the comments)

Submit

All Polls

Reports



[Strategic Security Report] Navigating the Threat Intelligence Maze

Most enterprises are using threat intel services, but many are still figuring out how to use the data they're collecting. In this Dark Reading survey we give you a look at what they're doing today - and where they hope to go.

Download Now!

The State of Ransomware **0 comments**

[Strategic Security Report] How Enterprises Are Attacking the IT Security Problem **0 comments**

The Impact of a Security Breach 2017 **0 comments**

More Reports

Twitter Feed

Cloud Distribution Retweeted

Cyren @CyrenInc

Number of Sites Hosting Cryptocurrency Miners Surges 725% in 4 Months darkreading.com/attacks-breach… via @DarkReading | #Cryptocurrency #Mining #Monero #DetectedByCyren

Number of Sites Hosting Cryptocurrency Miners Surges 725% in 4 Months

The dramatic increase in cryptocurrency prices, especially for Monero, is behind the sudden explosive gro…

darkreading.com

17h

ArkangelScrap Retweeted

ipfconline @ipfconline1

How Innovative Companies Lock Down Databuff.ly/2pO4Dzr by @JustinSomaini v/ @DarkReading#BigData #CyberSecurity #MachineLearning #Cognitive

Bug Report

Enterprise Vulnerabilities
From DHS/US-CERT's National Vulnerability Database

CVE-2017-0290
Published: 2017-05-09
NScript in mpengine in Microsoft Malware Protection Engine with Engine Version before 1.1.13704.0, as used in Windows Defender and other products, allows remote attackers to execute arbitrary code or cause a denial of service (type confusion and application crash) via crafted JavaScript code within ...

CVE-2016-10369
Published: 2017-05-08
unixsocket.c in lxterminal through 0.3.0 insecurely uses /tmp for a socket file, allowing a local user to cause a denial of service (preventing terminal launch), or possibly have other impact (bypassing terminal access control).

CVE-2016-8202
Published: 2017-05-08
A privilege escalation vulnerability in Brocade Fibre Channel SAN products running Brocade Fabric OS (FOS) releases earlier than v7.4.1d and v8.0.1b could allow an authenticated attacker to elevate the privileges

of user accounts accessing the system via command line interface. With affected version...

CVE-2016-8209
Published: 2017-05-08
Improper checks for unusual or exceptional conditions in Brocade NetIron 05.8.00 and later releases up to and including 06.1.00, when the Management Module is continuously scanned on port 22, may allow attackers to cause a denial of service (crash and reload) of the management module.

CVE-2017-0890
Published: 2017-05-08
Nextcloud Server before 11.0.3 is vulnerable to an inadequate escaping leading to a XSS vulnerability in the search module. To be exploitable a user has to write or paste malicious content into the search dialogue.

DARKReading

About Us
Contact Us
Sitemap
Reprints

Twitter
Facebook
LinkedIn
Google+
RSS

UBM

Technology Group

Black Hat
Content Marketing Institute
Content Marketing World
Dark Reading
Enterprise Connect
GDC
Gamasutra
HDI
ICMI
InformationWeek
INsecurity
Interop ITX
Network Computing
No Jitter
Service Management World
VRDC

COMMUNITIES SERVED

Content Marketing
Enterprise IT
Enterprise Communications
Game Development
Information Security
IT Services & Support

WORKING WITH US

Advertising Contacts
Event Calendar
Tech Marketing
Solutions
Contact Us
Licensing

Terms of Service | Privacy Statement | Legal Entities | Copyright © 2018 UBM, All rights reserved